UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF LOUISIANA

SHREVEPORT DIVISION

UNITED STATES OF AMERICA

VERSUS

$802,588.00 IN BANK FUNDS IN CATHAY BANK ACCOUNT ENDING IN 4278; $210,677.92 IN BANK FUNDS IN JP MORGAN CHASE ACCOUNT ENDING IN 3631; AND $32,225.27 IN BANK FUNDS IN JP MORGAN CHASE ACCOUNT ENDING IN 2671

VERIFIED COMPLAINT FOR FORFEITURE IN REM

Plaintiff, the United States of America, through the undersigned Assistant United States Attorney, brings this claim against the defendants identified herein collectively as the "defendant funds", and alleges as follows:

JURISDICTION AND VENUE

1. The Government brings this *in rem* civil forfeiture action pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C) and 984.

2. This Court has jurisdiction over the matter pursuant to 28 U.S.C. §§ 1345 and 1355.

3. Venue lies in this district pursuant to 28 U.S.C. § 1395.

PERSONS AND ENTITIES

4. The plaintiff in this action is the United States of America.

5. The defendant funds consist of the following:

a. $802,588.00 in bank funds seized pursuant to a federal seizure warrant on March 25, 2024, from a Cathay Bank account with the last four digits ending in 4278 ("Cathay Bank Account 4278"), held in the name of Stone Water Trading, LLC and seized at Cathay Bank, 4128 Temple City Blvd., Rosemead, CA 91770;

b. $210,677.92 in bank funds seized pursuant to a federal seizure warrant on March 24, 2024, from a JP Morgan Chase Bank account with the last four digits ending in 3631 ("Chase Bank Account 3631"), held in the name of STKG Consulting, Inc. and seized at JP Morgan Chase Bank, 3901 Atlantic Avenue, Long Beach, CA 90807; and

c. $32,225.27 in bank funds seized pursuant to a federal seizure warrant on March 24, 2024, from a JP Morgan Chase Bank account with the last four digits ending in 2671 ("Chase Bank Account 2671"), held in the name of JinLing Garment Trading, Inc. and seized at JP Morgan Chase Bank,3901 Atlantic Avenue, Long Beach, CA 90807.

6. The defendant funds are currently in the custody of the United States Secret Service ("USSS") and the Government will seek an arrest warrant *in rem* from the Clerk of Court so that the defendant funds will remain subject to this Court's jurisdiction during the pendency of this action.

7. The interests of Stone Water Trading, LLC, STKG Consulting, Inc., and JinLing Garment Trading, Inc. may be adversely affected by these proceedings.

BASIS FOR FORFEITURE

Background on Confidence Frauds

8. A "confidence fraud" involves a victim transferring money and/or property as a result of being deceived or misled by the offender. Often a fraudster deceives a victim into believing they have a close relationship—whether familial, friendly, or romantic—and leverages that relationship to persuade the victim to send money, provide personal and financial information, and/or purchase items of value.

9. Victims of confidence frauds often do not recognize that they are being defrauded for many months or more, and sometimes never recognize that they have been defrauded, because they are, or believe they are, in a legitimate relationship with the person making the false claims or promises to them. Therefore, it is not uncommon to observe multiple wires and transfers being sent to the same beneficiary or multiple beneficiaries over a period of time. Some victims of confidence frauds are not completely truthful with, or seek to impede, law enforcement officers who question them about the money they have transferred, in part to protect their purported friend.

10. Sometimes digital currency, also known as "crypto currency", "Cryptocurrency", and "virtual currency", is used in confidence frauds. Digital currency is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e. currency created and regulated by a government), but unlike fiat currency, has no physical form and instead exists entirely on the internet. In addition, digital currency is generated and controlled through computer

software operating on a decentralized peer-to-peer network. Digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership, or control of illegally obtained criminal proceeds.

11. A digital currency exchange (an "exchange") is a brick-and-mortar or online business that allows customers to trade digital currencies for fiat currencies or other digital currencies. Most exchanges are located outside the United States in order to avoid regulation and legal requirements.

The Law Enforcement Investigation in this Case

12. The USSS has investigated a confidence fraud whereby multiple victims transferred funds based on fraudulent pretenses directly into the accounts from which the defendant funds were seized. As part of the investigation, the USSS learned the information set forth below.

Victim 1 is Defrauded

13. In September 2023, Victim 1, a resident of Bossier City, Louisiana, was contacted via email on the website Facebook.com ("Facebook") by a person who went by Dora Richards ("Richards"). Richards and Victim 1 emailed each other regularly from September 2023 to February 2024; they never spoke on the phone or met in person. Richards told Victim 1 she owned a furniture wholesale store in Austin, Texas.

14. After several months of communicating, Richards brought up the topic of crypto currency investing. Richards told Victim 1 she was an investor and had earned significant trading profits. Richards encouraged Victim 1 to invest as well. At

first, Victim 1 was hesitant to invest but Richards told Victim 1 that she could provide him trading advice and convinced him to open an account on the crypto currency website PFT-AI.net. Victim 1 decided to invest in September 2023 and obtained wire transfer instructions via email from a customer service representative on the PFT-AI.net website.

15. From September 2023 to January 2024, Victim 1 sent a total of seven wire transfers totaling $675,000.00, including $250,200.00 to Cathay Bank Account 4278 on November 28, 2023, to accounts at JP Morgan Chase Bank, Cathay Bank, and MVB Bank. Victim 1 requested a $150,000.00 withdrawal of funds from his account at PFT-AI.net on February 5, 2024, and has not received any funds. Victim 1 contacted a representative of PFT-AI.net to inquire when the funds would be sent and was told his request was "in process and they are working on it."

Victim 2 is Defrauded

16. In June 2023, Victim 2, a resident of Leoma, Texas, received an unsolicited text message from a person who went by the name Lilia Ivanova ("Ivanova"). Over the next several months, Victim 2 and Ivanova communicated daily via text message. Ivanova sent Victim 2 a purported photo of herself and told him she owned a cosmetic company and lived in Newport, California. Victim 2 described Ivanova as an attractive Asian female in her 30s.

17. In July 2023, Ivanova told Victim 2 she has an aunt who was experienced in trading options and crypto currency and that she had earned significant investment returns. Ivanova told Victim 2 that he too should invest and

advised him to open an account on the website Pokadotex.net. Ivanova explained to Victim 2 that his investment funds would be used in short sell options with purchases and sales occurring in five-minute intervals.

18. From July 2023 to August 2023, Victim 2 made the following wire transfers: 1) on July 19, 2023, $20,000.00 to Chase Bank Account 3631; 2) on August 4, 2023, $65,344.00 to a Cathay Bank account in the name of Penguyan, Inc. with an account number ending in 5543 ("Penguyan 5543"); 3) on August 16, 2023, $30,090.00 to a JP Morgan Chase Bank account in the name of Stone Water, LLC with an account number ending in 1823 ("Chase Bank Account 1823"). Victim 2 was provided bank routing wire information by a customer service representative of Pokadotex.net and was told that he must send his wire transfers within two hours of receiving the banking information.

19. After these initial transfers, Victim 2 checked his account on Pokadotex.net and learned his balance was purportedly worth $800,000.00. Victim 2 told Ivanova of the returns he earned, and she explained to him that he could earn significantly more money, by upgrading his account on Pokadotex.net. Victim 2 was interested in upgrading his account and contacted customer service on Pokadotex.net and was told he would have to send $304,000.00 to meet the account upgrade capital requirements. Victim 2 told Ivanova he would like to upgrade his account but did not have more money to invest. Ivanova told Victim 2 that if he came up with some of the funds, she would cover the remaining balance.

20. In August 2023, Victim 2 obtained two loans and sent the following wire transfers: 1) on August 28, 2023, $225,000.00 to Chase Bank Account 1823; and 2) on September 27, 2023, $50,000.00 to Chase Bank Account 2671.

21. After sending the last $275,000.00 in wire transfers, Victim 2 asked Ivanova if she sent the remaining amount to cover the account upgrade. Ivanova told Victim 2 that any remaining funds she had available were used to care for her sick father. Victim 2 then contacted a customer service representative of Pokadotex.net to request a withdrawal of his funds but was told that his account will remain frozen until the remaining upgrade fees are received. No withdrawal of the purported funds has been allowed.

Victim 3 is Defrauded

22. In March 2023, Victim 3, a resident of Methuen, Massachusetts, received an unsolicited text message by a person who went by the name Emma Grace Aurora ("Aurora"). Over the next several months, Victim 3 and Aurora communicated daily via text message, speaking on the phone, or via Facetime. Aurora told Victim 3 that she was originally from Thailand but now lives in Beverly Hills, California. At first, Victim 3 considered this relationship with Aurora to be a friendship, but after a few months of communicating, Victim 3 felt that a romantic relationship was developing. Aurora and Victim 3 often talked about plans for their future and Aurora asked Victim 3 to visit her in Beverly Hills, California, over the 2023 Christmas holiday.

23. In June 2023, Aurora told Victim 3 that he earned a significant capital return by investing in crypto currency and advised Victim 3 that he should invest as well. Aurora instructed Victim 3 to download a crypto currency trading application called "ENKUU" from the Apple app store. Victim 3 agreed to invest and download the ENKUU app. Victim 3 received bank routing instructions via text message from an ENKUU customer service representative and was provided different bank and account names to where funds were to be sent. Victim 3 was told wire transfers must be sent within two hours of receiving this account information.

24. From July 2023 through August 2023, Victim 3 wire transferred the following: 1) on July 7, 2023, $10,000.00 to Chase Bank Account 1823; 2) on July 7, 2023, $10,000.00 to an MVB Bank account ending in 4209 in the name of Pay Wood Ventures, Inc. ("Pay Wood Account 4209"); 3) on July 20, 2023, $10,000.00 to Pay Wood Account 4209; 4) on July 20, 2023, $10,000.00 to an East West Bank account ending in 1568 in the name of Water Stone, Ltd.; 5) on August 2, 2023, $100,000.00 to Penguyan 5543; 6) on August 11, 2023, $20,000.00 to a Cathay Bank account ending in 4050 in the name of LCE Pure, Inc.; and 7) on August 18, 2023, $20,000.00 to Chase Bank account 1823.

25. Victim 3 checked his account on the ENKUU website and learned his balance was now purportedly worth $242,418.00. Victim 3 requested a funds withdrawal from his account and was told he must first pay a $37,000.00 "verification fee" to prove his identity or his account would be frozen. No withdrawal of the purported funds has been allowed.

Victim 4 is Defrauded

26. In August 2023, Victim 4, a resident of Jamaica Plain, Massachusetts, participated in internet chat groups related to music production sites. One of these groups was on Facebook. Through one of these sites, Victim 4 was contacted by a female who went by the name Gogo ("Gogo"). Gogo told Victim 4 she was from China, was now living in Chicago, Illinois, and owned an import/export furniture business. Gogo sent Victim 4 a photo purportedly of herself, and Victim 4 described her as a "very attractive Asian." Victim 4 and Gogo never met in person and communication was via internet communication applications Telegram and WhatsApp.

27. Gogo told Victim 4 she has a rich uncle who was a successful trader of crypto currency called Tether and could teach Victim 4 how to trade. Victim 4 was told to create accounts on the following websites: Enkuuex, DEX, and Morningstar. Victim 4 decided to invest and wire transferred funds from his account at Bank of America. Victim 4's understanding was that his funds were being used to purchase crypto currency, which would then be transferred to crypto currency trading sites. After investing his funds, Victim 4's accounts purportedly showed significant return on investments.

28. From June 2023 through August 2023, Victim 4 wire transferred the following: 1) on June 27, 2023, $200,000.00 to Chase Bank Account 3631; 2) on July 17, 2023, $130,000.00 to Chase Bank Account 3631; and 3) on August 9, 2023, $100,000.00 to Chase Bank Account 1823.

29. Victim 4 attempted to withdraw $200,000.00 of funds from one of his accounts, however, he was told he needed to pay a fee. Victim 4 began to believe he was a victim of a fraud scheme, when after paying the fee, he was then asked to pay a different set of fees. A DEX customer service representative told Victim 4 he must pay a $50,000.00 verification fee within five days or his account will be permanently restricted. No withdrawal of the purported funds has been allowed.

Tracing Fraud Proceeds into Cathay Bank Account 4278, Chase Bank Account 2671, and Chase Bank Account 3631

30. The following fraudulent proceeds, described above, were deposited into Cathay Bank Account 4278, Chase Bank Account 2671, and Chase Bank Account 3631:

a. On July 19, 2023, a $20,000.00 wire transfer to Chase Bank Account 3631; and on September 27, 2023, a $50,000.00 wire transfer sent to Chase Bank Account 2671, both from Victim 2 (see paragraphs 18 and 20 above);

b. On November 28, 2023, a $250,000.00 wire transfer sent to Cathay Bank Account 4278 from Victim 1 (see paragraph 15 above); and

c. On June 27, 2023, a $200,000.00 wire transfer sent to Chase Bank Account 3631; and on July 17, 2023, a $130,000.00 wire transfer sent to Chase Bank Account 3631; both from Victim 4 (see paragraph 28 above).

31. In addition, the USSS has identified additional suspicious deposits into the three seized accounts but has been unsuccessful in contacting and interviewing the individuals associated with the deposits/transfers who are believed to be victims of this scheme. These other presumed victims made approximately $2,271,484.00 in

suspicious deposits into the three accounts (the "Additional Deposits"). Of the $2,271,484.00 in Additional Deposits, approximately $552,465.00 was deposited into Cathay Bank Account 4278, approximately $500,412.00 was deposited into Chase Bank Account 2671, and approximately $1,218,607.00 was deposited into Chase Bank Account 3631.

32. The Additional Deposits share similarities with the above-described fraud victim transfers into the three seized accounts, in that they (1) were made in the same time period as the above-described transfers of fraud proceeds; (2) were made from individuals in locations throughout the United States without the kind of geographic patterns that might be expected from a legitimate business; (3) were made from people who had not previously deposited funds in the accounts; and (4) were almost entirely made in large round-dollar amounts, which are inconsistent with normal business transfers which typically reflect taxes and other costs). Accordingly, the Additional Deposits are also fraud proceeds from the victims of this scheme.

33. The Government seized $802,588.00 from Cathay Bank Account 4278. The specified transfer from Victim 1 described above, which totals $250,000.00, combined with the Additional Deposits, which total $552,465.00, represent a total of $802,665.00 of fraud proceeds traced into Cathay Bank Account 4278, which exceeds the amount the Government seized.

34. The Government seized $32,225.27 from Chase Bank Account 2671. The specified transfer from Victim 2 described above, which totals $50,000.00, combined with the Additional Deposits, which total $500,412.00, represent a total of

$550,412.00 of fraud proceeds traced into Chase Bank Account 2671, which exceeds the amount the Government seized.

35. The Government seized $210,677.92 from Chase Bank Account 3631. The specified transfers from Victims 2 and 4 described above, which total $350,000.00, combined with the Additional Deposits, which total $1,218,607.00 represent a total of $1,568,607.00 of fraud proceeds traced into Chase Bank Account 3631, which exceeds the amount the Government seized.

FIRST CLAIM FOR RELIEF

36. Based on the facts set out above, plaintiff, United States of America, alleges that the defendant funds constitute or are derived from proceeds traceable to violations of 18 U.S.C. § 1343, wire fraud, which is a specified unlawful activity as defined in 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1). The defendant funds are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C). In addition, to the extent that the defendant funds are not the actual monies directly traceable to the illegal activity identified herein, plaintiff alleges that the defendant funds are identical property found in the same account or place as the property involved in the specified offense, rendering the defendant funds subject to forfeiture pursuant to 18 U.S.C. § 984.

SECOND CLAIM FOR RELIEF

37. Based on the facts set out above, plaintiff, United States of America, alleges that the defendant funds constitute property involved in multiple transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(B)(i), or property

traceable to such property, with the specified unlawful activity being a violation of 18 U.S.C. § 1343, wire fraud. The defendant funds are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A). In addition, to the extent that the defendant funds are not the actual monies directly traceable to the illegal activity identified herein, plaintiff alleges that the defendant funds are identical property found in the same account or place as the property involved in the specified offense, rendering the defendant funds subject to forfeiture pursuant to 18 U.S.C. § 984.

THIRD CLAIM FOR RELIEF

38. Based on the facts set out above, plaintiff, United States of America, alleges that the defendant funds constitute property involved in multiple transactions or attempted transactions in violation of 18 U.S.C. § 1957(a), or property traceable to such property, with the specified unlawful activity being a violation of 18 U.S.C. § 1343, wire fraud. The defendant funds are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A). In addition, to the extent that the defendant funds are not the actual monies directly traceable to the illegal activity identified herein, plaintiff alleges that the defendant funds are identical property found in the same account or place as the property involved in the specified offense, rendering the defendant funds subject to forfeiture pursuant to 18 U.S.C. § 984.

WHEREFORE, plaintiff United States of America prays that:

(a) due process issue to enforce the forfeiture of the defendant funds;

(b) due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed;

(c) this Court decree of forfeiture of the defendant funds to the United States of America for disposition according to law; and

(d) for such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

ALEXANDER C. VAN HOOK
Acting United States Attorney

/s/ Lauren L. Gardner
LAUREN L. GARDNER, LA# 30595
Assistant United States Attorney
800 Lafayette Street, Suite 2200
Lafayette, LA 70501
Telephone: (337) 262-6618

VERIFICATION

I, Fred Apodaca, hereby declare that:

1. I am a Special Agent with the United States Secret Service.

2. I have read the above Verified Complaint for Forfeiture *In Rem* and know its contents. It is based upon my own personal knowledge and reports provided to me by other law enforcement agents.

3. Everything contained in the Complaint is true and correct, to the best of my knowledge and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed February 25, 2025, in Los Angeles, California.

Fred Apodaca

FRED APODACA
Special Agent